CLAIMS

What is claimed is:

1.   A method for permitting encrypted communications between two stations which are operable with compatible encryption algorithms that accept encryption keys having work factors with respectively different values, comprising:

in a first determining step, determining the lower one of the different work factor values;

providing an initial encryption key having a first work factor value;

comparing the first work factor value with the lower one of the work factor values determined in said determining step;

when, in said comparing step, the first work factor value is found to be greater than the lower one of the work factor values determined in said determining step, performing the following steps:

performing a hash function on a first word that includes the initial encryption key to produce an intermediate key, and deriving from the intermediate key a modified intermediate key having a work factor value not greater than the lower one of the different work factor values determined in said determining step;

performing a hash function on a second word that includes the modified intermediate key to produce a second output, and deriving from the second output a final encryption key having a work factor value not greater than the lower one of the different work factor values determined in said determining step; and

using the final encryption key to encrypt communications between the two stations.

2.   Apparatus for permitting encrypted communications between two stations which are operable with compatible encryption algorithms that accept encryption keys having work factors with respectively different values, comprising:

means for determining the lower one of the different work factor values;

means for providing an initial encryption key having a given work factor value;

means for comparing the first work factor value with the lower one of the work factor values;

means for performing a hash function on a first word that includes the initial encryption key to produce an intermediate key, and deriving from the intermediate key a

modified intermediate key having a work factor value not greater than the lower one of the different work factor values;

means for performing a hash function on a second word that includes the modified intermediate key to produce a second output, and deriving from the second output a final encryption key having a work factor value not greater than the lower one of the different work factor values; and

means for using the final encryption key to encrypt communications between the two stations if the first work factor value is found to be greater than the lower one of the work factor values.

3.   A method for permitting encrypted communications between two stations which are operable with compatible encryption algorithms that accept encryption keys having work factors with respectively different values, comprising:

determining a lowest one of the different work factor values;

providing an initial encryption key with a given work factor value;

comparing the given work factor value with the lowest one of the different work factor values; and

wherein, if the given work factor value is greater than the lowest one of the different work factor values, the method further comprises:

deriving from the initial encryption key a final encryption key having a work factor value not greater than the lowest one of the different work factor values; and

using the final encryption key for the encrypted communications.

4.   The method of claim 3, further comprising:

performing a first hash function on a first word that includes the initial encryption key to produce an intermediate key having a given length determined by the first hash function, and deriving the final encryption key from the intermediate key.

5.   The method of claim 4, wherein the first word comprises a combination of the initial encryption key and a salt.

6.   The method of claim 4, wherein if the given work factor is greater than the lowest one of the different work factor values, the method further comprises:

deriving from the intermediate key a modified intermediate key having a work factor value not greater than the lowest one of the different work factor values; and

deriving from the final encryption key from the modified intermediate key.

7.   The method of claim 6, further comprising:

performing a second hash function on a second word that includes the modified intermediate key to produce a second output; and

deriving from the second output the final encryption key.

8.   The method of claim 7, wherein the second word is combination of the intermediate key and a salt.

9.   The method of claim 7, wherein the second hash function is different from the first hash function.

10.   The method of claim 6, wherein deriving the modified intermediate key comprises:

setting a selected number of the most significant bit values of the intermediate key to zero.

11.   The method of claim 10, wherein the selected number is equal to a number resulting from subtracting the lowest one of the different work factor values from the given length of the intermediate key.

12.   The method of claim 3, wherein if the given work factor value is not greater than the lowest one of the different work factor values, the method further comprises:

using the initial encryption key for the encrypted communications.

13.   A method for permitting encrypted communications between two stations which are operable with compatible encryption algorithms having an accepted key length, wherein the encryption algorithms accept encryption keys having work factors with respectively different values, comprising:

generating an initial encryption key;

determining a lowest one of the different work factor values;

comparing the accepted key length and the lowest one of the different work factor values; and

wherein, if the lowest one of the different work factor values is less than the accepted key length, the method further comprises:

deriving from the initial encryption key a final encryption key having a work factor value not greater than the lowest one of the different work factor values; and

using the final encryption key for the encrypted communications.

14.   The method of claim 13, further comprising:

performing a first hash function on a first word that includes the initial encryption key to produce an intermediate key having a given length determined by the first hash function, and deriving the final encryption key from the intermediate key.

15.   The method of claim 14, wherein the first word comprises a combination of the initial encryption key and a salt.

16.   The method of claim 14, wherein if the lowest one of the different work factor values is less than the accepted key length, the method further comprises:

deriving from the intermediate key a modified intermediate key having a work factor value not greater than the lowest one of the different work factor values; and

deriving from the final encryption key from the modified intermediate key.

17.   The method of claim 16, further comprising:

performing a second hash function on a second word that includes the modified intermediate key to produce a second output; and

deriving from the second output the final encryption key.

18.   The method of claim 17, wherein the second word is combination of the intermediate key and a salt.

19.   The method of claim 17, wherein the second hash function is different from the first hash function.

20.   The method of claim 16, wherein deriving the modified intermediate key comprises:

setting a selected number of the most significant bit values of the intermediate key to zero.

21.   The method of claim 20, wherein the selected number is equal to a number resulting from subtracting the lowest one of the different work factor values from the given length of the intermediate key.

22.   The method of claim 13, wherein if the lowest one of the different work factor values is greater than the accepted key length, the method further comprises:

using the initial encryption key for the encrypted communications.

23.   The method of claim 22, wherein using the initial encryption key comprises:

using a selected number of the least significant bits of the initial encryption key, wherein the selected number is equal to the accepted key length.